STATE OF MONTANA
ice of the Legislative Auditor

EDP Audit

MAINFRAME COMPUTER SECURITY
DEPARTMENT OF ADMINISTRATION

PLEASE RETURN

This report contains conclusions and recommendations directed at security over information stored or processed on the state's mainframe computers. The recommendations include:

► Defining the computer security responsibilities of state agencies.

► Developing guidelines concerning suspending computer access.

► Establishing stricter controls over passwords.

► Developing and encouraging computer security training.

85DP-42

EDP AUDITS

Electronic data processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess state government operations. From the audit work, a determination is made whether agencies have adequate controls in their data processing systems, whether agency data processing operations are accomplishing their purposes, and whether they can do so with greater efficiency and economy. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office and the American Institute of Certified Public Accountants.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. One member is a Certified Information Systems Auditor and the other is a Certified Public Accountant.

EDP audits are performed at the request of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

EDP AUDIT REPORT

MAINFRAME COMPUTER SECURITY

November 1985

Report Number 85DP-42

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
HELENA, MONTANA 59620
406/444-3122

DEPUTY LEGISLATIVE AUDITORS:

JAMES GILLETT
FINANCIAL-COMPLIANCE AUDITS

JIM PELLEGRINI
PERFORMANCE AUDITS

LEGAL COUNSEL:

JOHN W. NORTHEY

SCOTT A. SEACAT
LEGISLATIVE AUDITOR

November 1985

The Legislative Audit Committee
of the Montana Legislature:

This is our EDP audit of security over information stored or processed on the state's mainframe computers, operated by the Information Services Division of the Department of Administration.

This report contains conclusions and recommendations concerning improvements to procedures for computer security. Department responses are contained at the end of the report.

We wish to express our appreciation to the staff of the department for their cooperation and assistance.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

TABLE OF CONTENTS

i

TABLE OF CONTENTS (Continued)

SUMMARY OF RECOMMENDATIONS

The following is a listing of recommendations of our EDP audit of security over information stored or processed on the state's mainframe computers. The major issues of this report relate to weaknesses in controls which allow access to programs and data. We also address the lack of adequate training for state agency management and personnel. We believe the problems identified in this report are due to no assigned responsibility for computer security.

Page

Recommendation #4

Technical Services Personnel not be assigned
unrestricted security authority.   14

Agency Response: Concur.   See page 23.

Recommendation #5

The Information Services Division issue
guidelines concerning the need for manage-
ment review of security reports.   14

Agency Response: Concur.   See page 23.

Recommendation #6

We recommend:
A.   The Installation Security Officer
     continue to schedule periodic
     training classes on various security
     related subjects.   17

Agency Response: Concur.   See page 24.

B.   The Information Services Division
     encourage agency management to enroll
     appropriate personnel in classes con-
     cerning computer security.   17

Agency Response: Concur.   See page 24.

Recommendation #7

The Legislature statutorily specify the
computer security responsibilities of
state agencies.   20

CHAPTER I

INTRODUCTION

As a result of recent audits expressing concern over computer security issues, the Legislative Audit Committee requested an EDP audit of information security at the state's major computer center. The audit was directed at security of information stored or processed on mainframe computers, an IBM 3033 and IBM 4381, operated by the Information Services Division of the Department of Administration.

AUDIT OBJECTIVES

The objectives of the EDP audit of mainframe security were:

1. To determine if security is adequate to protect agency data.

2. To evaluate the role and responsibilities of agency security officers and the division's Installation Security Officer.

3. To determine if security measures are reasonably implemented.

4. To determine if those responsible for agency security are adequately informed of security measures available and security policy established by the division.

SCOPE OF AUDIT

We identified various security systems available to protect information and ways access can be gained to information stored or processed at the state's computer center. We reviewed the organizational structure of the security function within the Information Services Division. We also examined how security policies are communicated and carried out in other state agencies.

We focused on installation and use of a computer system security product named "ACF2", the state's primary security mechanism. We examined policies and procedures relating to data

and program security. We also tested the adequacy of security measures currently used by state agencies.

COMPLIANCE

We did not find laws and policies relating to mainframe computer security. Nothing came to our attention that would indicate significant instances of noncompliance with any other laws or policies.

RECOMMENDATION FOR FUTURE AUDIT

The Information Services Division plans to rely primarily on ACF2 to provide protection over computer system resources and data. The division is currently installing ACF2 protection over the Customer Information Control System and is planning to install ACF2 to protect the Integrated Data Management System. Because of the planned reliance on ACF2, we did not test the current security programs being used for these systems.

The Integrated Data Management System is used to process central payroll transactions. The Customer Information Control System is used to process Medicaid information for the Department of Social and Rehabilitation Services, Motor Vehicle information for the Department of Justice, and information received from Uniform Commercial Code filings submitted to the Secretary of State's Office.

Because this is a transition period, we recommend an EDP audit be done of security control over information processed by these two systems at a later date. This later audit would be directed at determining the role and responsibilities of the users and the adequacy of implementing the security system.

CHAPTER II

BACKGROUND

SECURITY SYSTEMS

ACF2 is a vendor supplied computer program which provides the ability to control initial access to the computer system and access to programs and data stored on the system. It is one of the leading information security products on the market. The features of ACF2 can provide excellent security.

Logon Process

Three pieces of information are necessary to gain access or "logon" to the central computer system. First, a user must enter an active identification number.

Second, a password must be entered. Passwords are created and controlled by each individual user of the computer. The password entered must match the password stored by ACF2 or the system will not allow access.

The third piece of information needed is an account number used to charge for computer time and services. Each state agency is assigned certain valid account numbers. ACF2 validates all of this information upon entry to the system.

Access Control

Access to programs and data on the computer system is controlled by ACF2. There are four protection levels for controlling access. They are: 1) Read, 2) Write, 3) Allocate, and 4) Execute. For each protection level the type of access allowed can be: 1) Prevent, 2) Log, or 3) Allow. The following illustration explains each level and access type.

ACF2 SECURITY OPTIONS

PROTECTION LEVELS: Read - ability to look at programs or
                      data.

                      Write - ability to change or update pro-
                      grams or data.

                      Allocate - ability to add or delete entire
                      programs or data.

                      Execute - ability to execute or use pro-
                      grams or data.

ACCESS TYPE (one allowed to each protection level):

                      Prevent - will not allow access

                      Log - will log or record access

                      Allow - will allow access

For example, assume we have data and programs stored on
the computer. ACF2 can be directed to allow only a person with
proper identification the ability to read or execute the programs
and to prevent the person from being able to change (write) or
allocate the information stored. Other users can be prevented
from any access to the information or can be allowed to read and
execute the programs or data, but the activity will be logged and
reported.

STATE SECURITY STRUCTURE

The Information Services Division is responsible for imple-
menting and maintaining the ACF2 system. It has been the di-
vision's philosophy to provide the direction and tools for security.
However, agencies are responsible for the amount and type of
security necessary to protect their information.

The division has assigned most of the responsibility of securi-
ty matters to the division's Installation Security Officer. The
Technical Services Section of the division has been assigned to

4

perform periodical maintenance to ACF2. In order to perform maintenance, two people in the Technical Services Section have unrestricted security privileges. A fourth division employee has unrestricted security privileges. This person serves as back-up for the Installation Security Officer.

Each agency with a significant amount of information being stored or processed on the central computer has appointed an agency security officer. The security officers are responsible for security within their respective agencies.

Responsibility of the Division and the Installation Security Officer

The division is responsible for coordination and control of computer system access. It is also responsible for developing and maintaining operation procedures, user manuals, and associated training for users.

The Installation Security Officer is responsible for security over the central mainframe computers. The officer reviews ACF2 violation reports for each agency daily. These reports contain information showing any unauthorized security violations and identifies the user responsible. Assistance is offered to the agencies when problems are evident. Other responsibilities include:

1. Training and assisting in the use of ACF2 security software.

2. Controlling assignment of logon identification numbers and associated privileges.

3. Updating the ACF2 system.

4. Distributing documentation and assisting agency security officers.

5. Acting as security officer for the Department of Administration.

6. Acting as security officer for all agencies not having a security officer function within their departments.

Agency Security Officer Responsibilities

Agency security officers are responsible for security activities within their respective agencies. Duties include controlling logon identification numbers, writing ACF2 security options to allow or deny individuals access to programs and data, and reviewing agency violation reports. New users are assigned identification numbers by the Installation Security Officer upon request by an agency security officer. The agency security officer has the responsibility of controlling identification numbers and has the ability to cancel, suspend, and reassign those numbers.

Security privileges are assigned to an agency security officer, and one alternate for each agency. A person with security privileges has unlimited access to all the agency's programs and data.

Logon identification numbers are usually associated with a person, but can be identified with a functional group within an agency. For example, CNXXXX could be assigned to the Water Rights Bureau of the Department of Natural Resources and Conservation. In this case, the agency security officer must be sure that shared logon identification numbers do not allow access to critical or sensitive agency data or programs.

CHAPTER III

ACCESS CONTROLS

LOGON IDENTIFICATION NUMBER CONTROL

In order to gain access to information stored in the central computer, a valid logon identification number must be identified to the system. Each identification number is requested by an agency security officer and assigned by the Installation Security Officer. The Installation Security Officer assigns identification numbers that are unique to the requesting agency and records the initial person it was assigned to and privileges allowed.

After initial assignment, the agency security officer is responsible for identification number control. The agency security officer is responsible for suspending or cancelling the associated identification numbers of personnel transferred or terminated. Unused numbers can be reassigned to other agency personnel. All reassignments are approved and controlled by the agency's security officer.

During our audit, we reviewed logon identification security procedures used by agency security officers. We found security control weaknesses related to suspension procedures and the reassignment of unused numbers.

Suspension of Logon Identification Numbers

We discovered seventy-three active identification numbers assigned to personnel no longer employed by the state of Montana. These individuals still had access to the state computer system and had the capability to change, alter or destroy programs and data. We found active identification numbers assigned to terminated employees for the Department of Institutions, the Employment Security Division, Office of the Legislative Fiscal Analyst and the Department of Natural Resources and Conservation.

Strong logon identification controls should include a strict termination policy requiring immediate suspension of identification

7

numbers upon termination. Active numbers after employee termination provide an opportunity for ex-employees to alter or destroy agency programs and data.

We also identified 190 logon identification numbers that had not been accessed within 60 days. We identified these numbers because we believed that these "infrequent" users of the computer system represent a higher security risk than active users. In fact, we found that the infrequent users are significantly more susceptible to intruders trying to guess passwords than other groups. We attempted to logon to the state's computer system by using trivial passwords for 23 of these infrequently used identification numbers. We were successful 15 times or 65 percent of the time. (For average users we used trivial passwords and gained access 37 percent of the time. See page 11 for further discussion.)

Those identification numbers we guessed passwords for provided access to information stored by the Department of Commerce, Department of Health, Department of Highways, Department of Institutions, Employment Security Division, Department of Revenue, and Department of State Lands.

We believe the Information Services Division should issue security guidelines to inform agency security officers of the need to suspend identification numbers when employees terminate or when numbers are not frequently used. The Installation Security Officer should periodically review identification numbers and suspend those not used within the past 90 days.

The division has agreed with our recommendation and have started a monthly review of logon identification numbers and will suspend those that have been inactive for 90 days. Division officials have also indicated that security guidelines will be issued concerning the need to suspend identification numbers when employees terminate or when numbers are not frequently used.

RECOMMENDATION #1

WE RECOMMEND THE INFORMATION SERVICES DIVISION:

A.   ISSUE GUIDELINES CONCERNING THE NEED TO SUS-
     PEND LOGON IDENTIFICATION NUMBERS WHEN EM-
     PLOYEES TERMINATE OR WHEN LOGON IDENTIFICA-
     TION NUMBERS ARE NOT FREQUENTLY USED.

B.   PERIODICALLY REVIEW LOGON IDENTIFICATION NUM-
     BER ACTIVITY AND SUSPEND THOSE LOGON IDENTIFI-
     CATION NUMBERS NOT USED WITHIN THE PAST 90
     DAYS.

Reassigned Logon Identification Numbers

Agency security officers often reassign logon identification numbers of terminated employees to new users. Since security officers are limited to information concerning their own agencies, they are unable to determine access logon identification numbers have to data outside of their own agencies. This creates a significant security risk. By being reassigned a previous identification number, a person could have access to another agency's data without permission. For example, we noted one agency reassigned a number that had access to payroll information without consulting the Installation Security Officer or Central Payroll.

We believe the security risk caused by the reassignment of identification numbers could be eliminated by notifying the Installation Security Officer before numbers are transferred. Based on this information, the officer can notify the appropriate agencies before reassignment. Division officials agree that an exposure exists and intend to require all reassignments of identification numbers to be performed solely by the Installation Security Officer.

RECOMMENDATION #2

WE RECOMMEND THE INFORMATION SERVICES DIVISION
DIRECT AGENCY SECURITY OFFICERS TO NOTIFY THE
INSTALLATION SECURITY OFFICER BEFORE LOGON IDENTI-
FICATION NUMBERS ARE TRANSFERRED.

PASSWORD CONTROLS

Individual computer users are responsible for periodically
changing their passwords and controlling their secrecy. Each user
is responsible for having a unique password. ACF2 allows the
Information Services Division to set certain parameters that define
the characters that can be used as passwords. For example, a
password must be a minimum of three characters and a maximum of
eight characters. Passwords are stored in such a way as to
prevent access from other users. Agency security officers have
the ability to change passwords within their agency. Therefore, if
someone forgets a password the security officer can change the
password to allow access.

Passwords are set to expire every 90 days. This means the
user must change the password to a new password within 90 days.
If a user with an expired password tries to access the computer,
ACF2 will allow the user one chance to change it. Otherwise, the
logon identification number will be suspended.

Attempts to access the system with an incorrect password are
logged and written on a violation report. The system will automat-
ically logoff a user who tries to logon three times with the wrong
password. The logon identification number will be suspended if
seven invalid attempts are made in one day. An agency security
officer must activate a suspended identification number before it
can be used again.

To examine security, we reviewed active logon identification
numbers and tested for the presence of trivial passwords and the
reasonableness of privileges assigned to each identification number.

10

Trivial Passwords

We attempted to access the computer system for a sample of logon identification numbers by using as the password: the first name, last name, or identification number for the user. We were successful for 47 out of 127 users tested.

Information Services Division guidelines and federal standards specify that the composition of characters that make up a password should be easy to remember but not easily guessed by intruders. By guessing the passwords for various logon identification numbers tested, we had the opportunity to read, alter, or destroy information critical to various state agencies. For example, we had complete access to all programs and data at the Department of Highways, Department of Livestock, Workers' Compensation Division, and the Secretary of State's Office. This information is susceptible to being read, deleted, or altered. Examples include the following information:

1) Secretary of State's Office
   - Corporation profit and loss statements
   - Trademark registration
   - Uniform Commercial Code filings

2) Department of Livestock
   - Brand ownership information
   - Mortgages attached to brands

3) Workers' Compensation Division
   - Medical payment information

4) Department of Highways
   - Contractor payments
   - Bid estimates
   - Data input to payroll system

An even greater security risk was identified when we were able to logon with identification numbers assigned to seven agency security officers. This allowed us to change ACF2 to provide update access to all programs and data for the Department of Institutions, Department of Highways, Department of State Lands, Department of Natural Resources and Conservation, Department of

Livestock, Secretary of State's Office, and Workers' Compensation Division.

Agency security officers are responsible for educating users about password controls. However, users have the responsibility to control their individual passwords. In addition, the Information Services Division has a program available to prevent users from assigning easy-to-guess passwords. At the present time, this program has not been activated.

"Maxday" Password Privilege

We reviewed the privileges assigned to each active logon identification number. We found that agency security officers had altered the "maxday" password attribute for 100 identification numbers. By altering the "maxday" password attribute, a user is able to assign one password and never change it. Often, the password assigned qualifies as a trivial password and is easily guessed. In fact, we attempted to gain access to 25 user areas with the "maxday" privilege altered. We were successful 14 times, giving us read and update access to information for three agencies including the Department of Commerce, Department of Highways and Department of Natural Resources and Conservation.

The state guideline is for individuals to change their password every 90 days. The shorter the lifetime of a valid password, the higher the security provided by the password system. Frequent changes of passwords minimize the risk of undetected access.

Conclusion

At the present time, agency security officers and individual users are responsible for password controls. We believe that the Information Services Division should provide more central controls over passwords. Specifically, the division should activate the ACF2 program which provides stricter control over the characters used for passwords. Parameters should also be set so the "maxday" password attribute cannot be altered by agency security officers.

Division officials have indicated that stricter controls over identification numbers and passwords will be implemented, effective with the implementation of the new release of ACF2. This should be completed sometime in November, 1985.

RECOMMENDATION #3

WE RECOMMEND THE INFORMATION SERVICES DIVISION:

A. ACTIVATE THE ACF2 PROGRAM WHICH PROVIDES STRICTER CONTROL OVER CHARACTERS USED FOR PASSWORDS.

B. SET PARAMETERS SO THE "MAXDAY" PASSWORD AT-TRIBUTE COULD NOT BE ALTERED.

SEPARATION OF DUTIES

Separation of duties is a basic control needed to assure that errors cannot be perpetrated and concealed by the same person. During our audit we noted two instances where security could be improved by the separation of duties.

Technical Services Duties

Technical Services' personnel of the Information Services Division are responsible for maintenance of ACF2 and implementation of changes to ACF2. Their duties also include maintenance and emergency fixes for agency programs. Two people in Technical Services have unlimited security privileges, which means they can change and write access rules for all agencies in order to allow update access to programs when they need it.

The duties of the Technical Services personnel and security personnel should be separated in order to avoid any improper program changes to ACF2. Currently, Technical Services' personnel have update access to all agency data and also maintain the security system that protects the data. Therefore, an exposure exists for undetected access to unauthorized data.

13

Technical Services personnel should not be allowed unrestricted security authority to make it more difficult for them to manipulate agency programs and data. During emergencies, authorization to agency data would be approved through security personnel. In addition, access for maintenance to ACF2 would be controlled by the Installation Security Officer.

RECOMMENDATION #4
WE RECOMMEND THAT TECHNICAL SERVICES PERSONNEL NOT BE ASSIGNED UNRESTRICTED SECURITY AUTHORITY.

Agency Security Officer's Duties

Agency security officers are responsible for providing access to agency data and reviewing ACF2 violation reports showing unauthorized activity. This creates a situation where the security officer can gain access, change, or delete data without detection. These duties should be separated in order to provide more effective access control.

We believe it would be more appropriate for department management to review violation and activity reports instead of the security officer. The Information Services Division should issue guidelines to agencies directed at the need to separate duties for adequate access control.

RECOMMENDATION #5
WE RECOMMEND THAT THE INFORMATION SERVICES DIVISION ISSUE GUIDELINES CONCERNING THE NEED FOR MANAGEMENT REVIEW OF SECURITY REPORTS.

SECURITY TRAINING AND AWARENESS

The Installation Security Officer is responsible for training agency personnel on use of the security system. Duties include teaching agency security officers how to use ACF2 to protect agency data and educating agency management about security responsibilities and awareness.

Security awareness is directed at agency management, as well as security officers. The Installation Security Officer has used personal contact and the the division's "News and Views" to address securities issues. The "News and Views" is a monthly publication distributed by the division to other state agencies discussing data processing issues.

Training classes were given to agency security officers when ACF2 was initially installed. The class gave a comprehensive description of ACF2, and how to use it to allow or deny access. Since then, training has been on an individual basis, as needed. An independent study course has been purchased by the division to help security officers learn ACF2 protection and programming procedures. The Installation Security Officer has been lending the course to agencies at their request. An updated version of ACF2 is being implemented, and when completed, the Installation Security Officer plans to offer formal classes to agencies interested.

Training Concerns

We found six agency security officers that have not attended formal training classes on ACF2. Because of inadequate training they were unaware that programming they had done did not adequately protect agency data.

For example, the Department of Highways attempted to limit update access to functional groups within the department. However, all personnel in the Department of Highways have the same update access.

In addition, we found six agencies that are not yet completely ACF2 protected from unauthorized access. All agencies should be in the ACF2 mode that protects agency data and programs. ACF2 can operate in three modes. The three modes are "log," "warn," and "cancel."

ACF2 MODE OPTIONS

System Mode Options: Log – will allow unauthorized access, but records the access.

Warn – will allow unauthorized access but issue a warning message to user and records the attempt.

Cancel – will not allow unauthorized access and records attempt.

There is a potential exposure for agency data to be altered or destroyed when operating in modes other than "cancel". At the time of our review the Department of Institutions stored Automated Billings and Accounts Receivable System (ABARS) data on the mainframe. Because this data was protected under a less than secure mode, anyone with a logon identification number had update access to the information.

The Installation Security Officer has informally offered to schedule classes for agency security officers, directed at how to use ACF2 to protect programs and data stored on the computer. However, not enough interest has been demonstrated to justify a class.

We believe the Installation Security Officer should continue to schedule classes on various security related subjects to be offered to agency security officers and agency management. The Information Services Division should encourage agency management to enroll appropriate personnel in scheduled classes concerning computer security.

RECOMMENDATION #6

WE RECOMMEND:

A. THE INSTALLATION SECURITY OFFICER CONTINUE TO
    SCHEDULE PERIODIC TRAINING CLASSES ON VARIOUS
    SECURITY RELATED SUBJECTS.

B. THE INFORMATION SERVICES DIVISION ENCOURAGE
    AGENCY MANAGEMENT TO ENROLL APPROPRIATE
    PERSONNEL IN CLASSES CONCERNING COMPUTER
    SECURITY.

17

CHAPTER V

MANAGEMENT OF INFORMATION SECURITY

The responsibility for management of security over state information processed and stored on computers is divided between the Information Services Division of the Department of Administration and agency management. The division has made available security software and developed procedures to protect data. Agency management has the responsibility to see that the procedures are used. During our audit of mainframe security, we identified several management control weaknesses.

Our audit work identified weaknesses in logon identification number and password security controls. These weaknesses included:

1. No transfer or termination policies;

2. Unused identification numbers are not suspended;

3. Identification numbers are reassigned without complete access information;

4. Assignment of trivial, easy-to-guess passwords; and

5. Privileges are altered so password changes are not required.

We identified areas where security training is needed. The following examples were noted:

.1. ACF2 procedures at agencies that did not adequately protect data.

2. Agencies operating under a less than secure mode.

Because of weaknesses in controls, state agencies are not adequately protected from data destruction, alteration, or theft. We believe these weaknesses exist because agency management has been lax in assigning and reviewing responsibilities. In addition, existing Montana law does not assign responsibility for the security of state information stored or processed on computers.

One state has taken steps to solve this problem by statutorily specifying the responsibilities of the central administering agency (Department of Administration) and the other agencies. Under this system, the Department of Administration would:

1. Establish and maintain the minimum security standards, rules and regulations necessary to implement a state agency security plan.

2. Establish guidelines to assist agencies in identifying electronic data processing personnel occupying positions of special trust or responsibility or sensitive locations.

3. Establish rules and regulations for the exchange of data between data centers or departments to ensure that exchanges do not jeopardize data security and confidentiality.

4. Coordinate and provide for a training program regarding security of data and information resources to serve governmental technical and managerial needs.

5. Provide technical and managerial assistance relating to the security program upon request.

Department directors would be given responsibility for assuring adequate security exists over data and computer resources. Specifically, they would be required to:

1. Designate an information security manager who shall administer the department's security program for data and information resources.

2. Conduct, and periodically update, a comprehensive risk analysis to determine the security threats to the data and information resources.

3. Develop, and periodically update, written policies and procedures to assure the security of the data and information resources.

4. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to the data and information resources.

5. Ensure that periodic internal audits and evaluations of the security program for data and information resources are conducted.

6. Include appropriate security requirements, as determined by the department, in the written specifications for the department's solicitation of information processing resources.

7. Certify annually to the Department of Administration that the security program conforms with the established standards, policies and guidelines developed. If the department is unable to certify its conformance, it shall notify the Department of Administration, in writing, stating the deficiencies and the reasons for nonconformance.

We believe this type of system would be advantageous for promoting computer security for state government. Thus, we recommend the Legislature define the computer security responsibilities of state agencies.

RECOMMENDATION #7

WE RECOMMEND THE LEGISLATURE STATUTORILY SPECIFY THE COMPUTER SECURITY RESPONSIBILITIES OF STATE AGENCIES.

AGENCY RESPONSE

TED SCHWINDEN GOVERNOR   MITCHELL BUILDING

STATE OF MONTANA

(406) 449-2032   HELENA MONTANA 59620

RECEIVED

NOV 2 5 ...

MONTANA LEGISLATIVE AUDITOR

November 25, 1985

Scott Seacat
Legislative Auditor
State Capitol
Helena, Montana 59620

Dear Mr. Seacat:

We have reviewed the recommendations for improving EDP
security. The recommendations should serve to improve
the existing situation. Our staff has already begun to
implement several of the recommendations.

Our responses to each of the recommendations are enclosed.
We appreciate the opportunity we have had to interact with
your staff on these issues.

Sincerely,

Ellen Feaver

ELLEN FEAVER
Director

Enclosures

RECOMMENDATION #1

WE RECOMMEND THE INFORMATION SERVICES DIVISION:

A. ISSUE GUIDELINES CONCERNING THE NEED TO SUSPEND LOGON IDENTIFICATION NUMBERS WHEN EMPLOYEES TERMINATE OR WHEN LOGON IDENTIFICATION NUMBERS ARE NOT FREQUENTLY USED.

B. PERIODICALLY REVIEW LOGON IDENTIFICATION NUMBER ACTIVITY AND SUSPEND THOSE LOGON IDENTIFICATION NUMBERS NOT USED WITHIN THE PAST 90 DAYS.

D OF A RESPONSE

We concur with this recommendation. We are requesting that Central Payroll provide the Installation Security Officer a list of all terminated employees on a biweekly basis. The Installation Security Officer will cancel LOGONIDS for all terminated employees on a ongoing basis. We have initiated a policy directing the Installation Security Officer to suspend LOGONIDS that have been inactive for 90 days once each month.

RECOMMENDATION #2

WE RECOMMEND THE INFORMATION SERVICES DIVISION DIRECT AGENCY SECURITY OFFICERS TO NOTIFY THE INFORMATION SECURITY OFFICER BEFORE LOGON IDENTIFICATION NUMBERS ARE TRANSFERRED.

D OF A RESPONSE

We concur with this recommendation. We have removed the ability of Agency Security Officers to reassign LOGONIDS entirely. This function will be limited to the Installation Security Officer only.

RECOMMENDATION #3

WE RECOMMEND THE INFORMATION SERVICES DIVISION:

A. ACTIVATE THE ACF2 PROGRAM WHICH PROVIDES STRICTER CONTROL OVER CHARACTERS USED FOR PASSWORDS.

B. SET PARAMETERS SO THE "MAXDAY" PASSWORD ATTRIBUTE COULD NOT BE ALTERED.

D OF A RESPONSE

We concur with this recommendation, and will further restrict the format and frequency of change of passwords as follows:

A. Trivial Passwords:

Concurrent with the new release of ACF2 the following changes will be implemented:

1. Minimum password length will be changed to four characters.

2. Both numeric and alphabetic characters will be required in each password.

B. MAXDAYS

The ability to change the MAXDAYS parameter will be limited to the Installation Security Officer. This will assure that all changes to this parameter are justified on a case by case basis.

RECOMMENDATION #4

WE RECOMMEND THAT TECHNICAL SERVICES PERSONNEL NOT BE ASSIGNED UNRESTRICTED SECURITY AUTHORITY.

D OF A RESPONSE

We concur with this recommendation. Unrestricted security authority will be removed from Technical Services Section personnel.

Two persons will be assigned this level of security; the Installation Security Officer and his backup.

On special occasions where unrestricted security authority is required to perform necessary system maintenance functions, the unrestricted security authority will be temporarily assigned by the Installation Security Officer. The activities will be controlled and monitored by the Installation Security Officer and removed upon completion of the specific maintenance.

RECOMMENDATION #5

WE RECOMMEND THAT THE INFORMATION SERVICES DIVISION ISSUE GUIDELINES CONCERNING THE NEED FOR MANAGEMENT REVIEW OF SECURITY REPORTS.

D OF A RESPONSE

We concur with this recommendation. Information Services Division will issue guidelines for agency management review of ACF2 security reports.

RECOMMENDATION #6

WE RECOMMEND:

A. THE INSTALLATION SECURITY OFFICER CONTINUE TO SCHEDULE PERIODIC TRAINING CLASSES ON VARIOUS SECURITY RELATED SUBJECTS.

B. THE INFORMATION SERVICES DIVISION ENCOURAGE AGENCY MANAGEMENT TO ENROLL APPROPRIATE PERSONNEL IN CLASSES CONCERNING COMPUTER SECURITY.

D OF A RESPONSE

We concur with this recommendation.

A. The Installation Security Officer will continue to provide periodic training classes on security related subjects.

B. Information Services Division will encourage user management to participate in computer security related classes.

> NOTE: Agency responsibility, participation, and involvement in security will be encouraged in future sessions of both the Data Processing Advisory Council and the Data Processing Managers Group.